

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Shinji KIKUCHI et al.

Application No.: Unassigned

Group Art Unit: Unassigned

Filed: (Concurrently)

Examiner: Unassigned

For: DEVICE FOR DETECTING FAILURE OF COMMUNICATION NETWORK

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Application No. 2003-296768

Filed: August 20, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 3/10/04

By: Richard A. Gollhofer
Richard A. Gollhofer
Registration No. 341,106

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: August 20, 2003

Application Number: Patent Application
No. 2003-296768

[ST.10/C]: [JP2003-296768]

Applicant(s) : FUJITSU LIMITED

December 22, 2003

Commissioner,
JAPAN Patent Office Yasuo IMAI

Certificate No. P2003-3106430

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 8月20日
Date of Application:

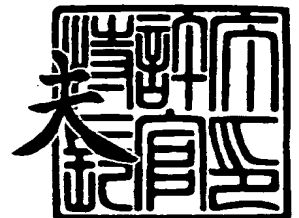
出願番号 特願2003-296768
Application Number:
[ST. 10/C]: [JP 2003-296768]

出願人 富士通株式会社
Applicant(s):

2003年12月22日

特許庁長官
Commissioner,
Japan Patent Office

今井 康



出証番号 出証特2003-3106430



【書類名】 特許願
【整理番号】 0351810
【提出日】 平成15年 8月20日
【あて先】 特許庁長官殿
【国際特許分類】 G06F 17/00
H04L 12/26

【発明者】
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社
内
【氏名】 菊池 慎司

【発明者】
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社
内
【氏名】 中原 浩之

【特許出願人】
【識別番号】 000005223
【氏名又は名称】 富士通株式会社

【代理人】
【識別番号】 100074099
【住所又は居所】 東京都千代田区二番町8番地20 二番町ビル3F
【弁理士】
【氏名又は名称】 大菅 義之
【電話番号】 03-3238-0031

【選任した代理人】
【識別番号】 100067987
【住所又は居所】 神奈川県横浜市鶴見区北寺尾7-25-28-503
【弁理士】
【氏名又は名称】 久木元 彰
【電話番号】 045-545-9280

【手数料の表示】
【予納台帳番号】 012542
【納付金額】 21,000円

【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9705047

【書類名】 特許請求の範囲**【請求項 1】**

複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出する障害検出装置であって、

前記監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を格納する格納手段と、

前記トラフィック流量情報を用いて、前記監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、得られた流量を異常トラフィック量として出力する計算手段と、

前記異常トラフィック量を用いて前記ネットワーク障害が発生したか否かを判定し、判定結果を出力する判定手段と

を備えることを特徴とする障害検出装置。

【請求項 2】

複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出するコンピュータのためのプログラムであって、

前記コンピュータの格納手段から、前記監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を取り出し、

前記トラフィック流量情報を用いて、前記監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、

得られた流量を異常トラフィック量として用いて前記ネットワーク障害が発生したか否かを判定する

処理を前記コンピュータに実行させることを特徴とするプログラム。

【請求項 3】

前記監視対象機器により生成されて出力されるデータのトラフィック量と、該監視対象機器により廃棄されるデータのトラフィック量と、該監視対象機器のインタフェースにより受信された後に同じインタフェースから送信されるデータのトラフィック量のうち少なくとも 1 つのトラフィック量を、前記異常トラフィック量として計算する処理を前記コンピュータに実行させることを特徴とする請求項 2 記載のプログラム。

【請求項 4】

前記監視対象機器の内部におけるトラフィックの総量に対する前記異常トラフィック量の比率を求め、該異常トラフィック量の比率が所定の閾値より大きい場合に前記ネットワーク障害が発生したと判定する処理を前記コンピュータに実行させることを特徴とする請求項 2 記載のプログラム。

【請求項 5】

前記監視対象機器の内部にトラフィックの終点および始点を表す仮想点を設け、該監視対象機器の内部において各インタフェースを始点とし他のインタフェースを終点とする第 1 のトラフィックの流量と、各インタフェースを始点とし該仮想点を終点とする第 2 のトラフィックの流量と、該仮想点を始点とし各インタフェースを終点とする第 3 のトラフィックの流量と、該監視対象機器の内部において各インタフェースを始点とし同じインタフェースを終点とする第 4 のトラフィックの流量を計算し、該第 2、第 3、および第 4 のトラフィックの流量の総量を前記異常トラフィック量として計算する処理を前記コンピュータに実行させることを特徴とする請求項 2 記載のプログラム。

【書類名】 明細書**【発明の名称】 通信ネットワークの障害を検出する装置****【技術分野】****【0001】**

本発明は、通信ネットワークにおけるトラフィックの流れを解析することによりネットワークの障害を検出する装置に関する。

【背景技術】**【0002】**

従来より、通信ネットワーク内の障害を検知するための技術としては、以下のようなものが知られている。

(A) エラーメッセージ捕捉

監視機器は、障害発生時にネットワーク機器が生成するエラーメッセージを観測し、生成されたエラーメッセージを捕捉したらアラームを出力して、ネットワーク管理者に障害の発生を通知する（例えば、非特許文献1参照）。

(B) パケットキャプチャ

ネットワーク内部に流れるパケットを捕捉し、それらのパケットを1つ1つ調査することにより、障害が発生しているかどうかを判定する（例えば、非特許文献2参照）。

【0003】

また、トラフィック行列 (Traffic Matrix) を用いたいくつかのネットワーク解析方法も知られている（例えば、非特許文献3および4参照）。

【0004】

【非特許文献1】 “Remote Network Monitoring Management Information Base ”、[online]、RFC 1757、[平成15年7月18日検索]、インターネット<URL : <http://www.faqs.org/rfcs/rfc1757.html>>

【非特許文献2】 “Sniffer Technologies (登録商標)”、[online]、Network Associates、[平成15年7月18日検索]、インターネット<URL : <http://www.nai.com/japan/products/sniffer/home.asp>>

【非特許文献3】 J. Cao, D. Davis, S. Vander Wiel, and B. Yu, “Time-Varying Network Tomography: Router Link Data”, Journal of the American Statistical Association, 2000

【非特許文献4】 C. Tebaldi and M. West, “Bayesian Inference on Network Traffic Using Link Count Data”, Journal of the American Statistical Association, 1998

【発明の開示】**【発明が解決しようとする課題】****【0005】**

しかしながら、上述した従来の障害検出方法には、次のような問題がある。

【0006】

上記 (A) の方法においては、例えば IP (Internet Protocol) ネットワークにおける ICMP (Internet Control Message Protocol) destination unreachable エラーや、ICMP time exceeded エラーを観測し、それらのエラーメッセージの発生の有無に基づいて障害の存在を確認する。

【0007】

しかし、これらのエラーメッセージを発生させない障害も多数存在する。また、これらのエラーメッセージは、ユーザによる経路調査ツール traceroute の実行や、アクセス時の宛先 IP アドレスの指定ミス等により、ネットワーク内に定常的に存在する。このようなことから、障害の程度が小さい場合には、これらのエラーメッセージの発生頻度も小さいため、これらのエラーメッセージの有無に基づいて障害の検知を行うのは一般的には困難である。

【0008】

また、上記(B)の方法においては、パケットキャプチャ機器を、障害が原因で発生するパケットが流れる場所に配置しなければならないため、広い範囲のネットワークを監視する場合、多数のパケットキャプチャ機器を配置する必要がある。また、全てのパケットデータを高速に大量に記録する必要があるため、そのためのリソース消費は多大である。このようなことから、パケットキャプチャを用いた障害検出方法はコストが非常に高くなるため、現実的な方法であるとは言えない。

【0009】

本発明の課題は、通信ネットワーク内で発生する障害を、その影響が比較的小さい早期のうちに低コストで検出する障害検出装置を提供することである。

【課題を解決するための手段】

【0010】

図1は、本発明の障害検出装置の原理図である。図1の障害検出装置は、格納手段101、計算手段102、および判定手段103を備え、複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出する。

【0011】

格納手段101は、監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を格納する。計算手段102は、トラフィック流量情報を用いて、監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、得られた流量を異常トラフィック量として出力する。判定手段103は、異常トラフィック量を用いてネットワーク障害が発生したか否かを判定し、判定結果を出力する。

【0012】

格納手段101は、例えば、後述する図3のトラフィック流量記録装置312および後述する図8のトラフィック流量記録装置801に対応する。計算手段102は、例えば、図3のトラフィック流量分析装置313および異常トラフィック量計算装置314と、図8のトラフィック流量分析装置802および異常トラフィック量計算装置803に対応する。判定手段103は、例えば、図3の障害判定装置315および図8の障害判定装置804に対応する。

【発明の効果】

【0013】

本発明によれば、容易に取得可能なトラフィック流量情報を分析し、そこから異常な流れ方を示すトラフィックの量を導出することにより、ネットワーク障害の有無が判定される。これにより、ネットワーク内で発生するエラーメッセージに頼ることなく、またネットワーク内に特別なパケットキャプチャ機器を配置することなく、ネットワーク内部を流れる異常トラフィックを識別することができる。したがって、広範囲な通信ネットワークにおいて、障害の影響が小さいうちに、その障害の発生を早期にかつ低コストで検出することが可能になる。

【発明を実施するための最良の形態】

【0014】

以下、図面を参照しながら、本発明を実施するための最良の形態を詳細に説明する。

【0015】

図2は、本発明を実施するためのネットワーク構成の例を示している。図2のネットワーク構成において、障害検出装置201は、通信ネットワーク内部における複数の中継機器等の監視対象機器202～207からトラフィック流量情報を収集し、それらの監視対象機器における障害の有無を判断する。ここでは、簡単のため6つの監視対象機器が示されているが、監視対象機器の数は一般に任意である。

【0016】

障害検出装置201は、図3に示すように、トラフィック流量取得装置311、トラフィック流量記録装置312、トラフィック流量分析装置313、異常トラフィック量計算

装置 314、および障害判定装置 315 を備え、ネットワーク内部の障害を検出する。監視対象機器 301 は、図 2 の監視対象機器 202 ~ 207 のいずれかに対応する。

【0017】

図 4 は、図 3 の障害検出装置 201 による障害検出処理のフローチャートである。図 4 の障害検出処理の手順は、以下のようになる。

ステップ 401：

トラフィック流量取得装置 311 は、監視対象機器 301 に対して、その監視対象機器 301 が保持しているトラフィック流量情報を要求するリクエストを送信する。そのリクエストに対して、監視対象機器 301 は、それが保持しているトラフィック流量情報を障害検出装置 201 に対して送信する。例えば、IP ネットワークの場合、このトラフィック流量情報としては、監視対象機器 301 の Management Information Base-II (MIB-II) データベースに保持されている、各インタフェースにおける入力／出力パケット数や、入力／出力オクテット数等が用いられる。また、トラフィック流量取得装置 311 が送出するリクエストとしては、Simple Network Management Protocol (SNMP) の get リクエスト等が用いられる。

ステップ 402：

トラフィック流量取得装置 311 が監視対象機器 301 のトラフィック流量情報を取得すると、トラフィック流量記録装置 312 は、その流量情報を記録する。

ステップ 403：

トラフィック流量分析装置 313 は、記録されたトラフィック流量情報を用いて、トラフィック流量の分析を行う。ここで行われる分析とは、ネットワーク内を流れる個々のパケットの保持するデータや挙動を調査するのではなく、トラフィックの大局的な流れを捉えることを言う。例えば、トラフィックが監視対象機器 301 のどのインタフェースから入力され、そのトラフィックがどのインタフェースから出力されるかを、各インタフェースにおけるトラフィック流量情報から推定する。

【0018】

例えば、監視対象機器 301 が 3 つのインタフェースを持つルータである場合、このルータは図 5 のようなモデルにより表現できる。このモデルにおいては、ルータは 3 つのインタフェース A、B、および C を持ち、それぞれのインタフェースにおける単位時間当たりの受信トラフィック量 (y_{in-A} , y_{in-B} , y_{in-C}) と送信トラフィック量 (y_{out-A} , y_{out-B} , y_{out-C}) が取得可能なトラフィック流量情報であるとする。

【0019】

また、ルータの内部には、ルータの内部で消滅するトラフィックの終点や、ルータが送信元となるようなトラフィックの始点に対応する仮想的な点を表す要素 O があるものとする。さらに、ルータの内部において、 α ($\alpha \in \{A, B, C, O\}$) を始点とし β ($\beta \in \{A, B, C, O\}$) を終点として流れるトラフィックの量を $x_{\alpha\beta}$ と記し、このルータで送受信される全てのトラフィックはいずれかの $x_{\alpha\beta}$ にカウントされるものとする。この場合、以下のような連立方程式が成り立つ。

【0020】

【数 1】

$$Y = \begin{pmatrix} Y_{in-A} \\ Y_{in-B} \\ Y_{in-C} \\ Y_{out-A} \\ Y_{out-B} \\ Y_{out-C} \end{pmatrix} \quad (1)$$

$$X = \begin{pmatrix} x_{AA} \\ x_{AB} \\ x_{AC} \\ x_{BA} \\ x_{BB} \\ x_{BC} \\ x_{CA} \\ x_{CB} \\ x_{CC} \\ x_{AO} \\ x_{BO} \\ x_{CO} \\ x_{OA} \\ x_{OB} \\ x_{OC} \end{pmatrix} \quad (2)$$

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (3)$$

$$Y = AX \quad (4)$$

【0021】

しかし、(4)式では、6個の方程式に対して、ルータ内部におけるトラフィックの流れを表す15個の未知数 $x_{\alpha\beta}$ が存在するので、この連立方程式を解析的に解くことはできない。そこで、トラフィック流量分析装置313は、単位時間当たりの受信トラフィック量(y_{in-A} , y_{in-B} , y_{in-C})と送信トラフィック量(y_{out-A} , y_{out-B} , y_{out-C})から各 $x_{\alpha\beta}$ の値を推定する。この推定には、例えば、前述した非特許文献3および4に示されているようなTraffic Matrix Estimation という方法を用いることができる。

ステップ404:

トラフィック流量分析装置313が監視対象機器301の各インタフェース間を流れるトラフィックを推定すると、異常トラフィック量計算装置314は、得られたトラフィックのうち監視対象機器301の目的にそぐわない異常なトラフィックの量を計算する。

【0022】

例えば、監視対象機器301がルータやスイッチ等の中継機器である場合、その機器の

主な目的は、外部から受信したデータを別の場所へ転送することである。したがって、この監視対象機器 301 により生成されて出力されるようなデータや、この機器で終端されて廃棄されるデータや、そのデータを受信したインタフェースから送信されるようなデータは、通常は非常に少ないはずである。このようなデータが大量に発生した場合には、何らかの障害が発生したと考えられる。

【0023】

そこで、異常トラフィック量計算装置 314 は、これらのデータの量を異常トラフィック量としてカウントし、それ以外のデータの量を正常トラフィック量としてカウントして、得られた正常／異常トラフィック量を障害判定装置 315 に転送する。

【0024】

図 5 のモデルの場合、トラフィック流量分析装置 313 により推定された $x_{\alpha\beta}$ のうち、 x_{AA} 、 x_{BB} 、 x_{CC} 、 x_{AO} 、 x_{BO} 、 x_{CO} 、 x_{OA} 、 x_{OB} 、および x_{OC} が異常トラフィック量としてカウントされる。 x_{AA} 、 x_{BB} 、および x_{CC} は、データを受信したインタフェースからそのデータが送信されるようなループトラフィックの量を表している。また、 x_{AO} 、 x_{BO} 、および x_{CO} は、ルータ内部で廃棄されるトラフィックの量を表し、 x_{OA} 、 x_{OB} 、および x_{OC} は、ルータ内部で生成されて出力されるトラフィックの量を表している。そこで、異常トラフィック量計算装置 314 は、これらのトラフィックの総量を計算する。

ステップ 405:

障害判定装置 315 は、異常トラフィック量計算装置 314 が算出した正常／異常トラフィック量に基づいて障害の有無を判定する。このとき、異常トラフィックの総量が、ネットワーク管理者等が指定した所定の閾値を超えた場合に、障害が発生したものと判断する。

【0025】

図 5 のモデルの場合、次式のような評価関数 $f(X)$ を用いて、ルータ内部のトラフィックの総量に対する異常トラフィック量の比率が計算される。

【0026】

【数 2】

$$f(X) = \frac{\sum_{\mu} (x_{\mu 0} + x_{0\mu} + x_{\mu\mu})}{\sum_{\mu} \sum_{\nu} x_{\mu\nu} + \sum_{\mu} (x_{\mu 0} + x_{0\mu})} \quad (5)$$

($\mu, \nu \equiv \{A, B, C\}$)

【0027】

(5) 式の右辺の分子は、異常トラフィックの総量を表す。また、(5) 式の右辺の分母は、トラフィックの総量を表し、正常トラフィックの総量と異常トラフィックの総量を加算することで得られる。障害判定装置 315 は、この $f(X)$ の値を所定の閾値と比較し、その値が閾値を超えれば障害が発生したものと判断する。例えば、許容可能な異常トラフィック量が全体のトラフィック量の 10% である場合、閾値は 0.1 に設定される。

ステップ 406:

障害判定装置 315 は、ステップ 405 において障害が発生したと判断した場合、アラームを出力してネットワーク管理者等に障害の発生を通知する。

【0028】

図 5 では 3 つのインタフェースを有するルータのモデルが示されているが、インタフェースの数がそれより多い場合も、同様のモデルを構築することで障害を検出することができる。

【0029】

また、ルータ等の中継機器以外の監視対象機器 301 としては、ファイアウォールやブ

ロキシサーバ等のように、ゲートウェイとしての役割を果たす機器が考えられる。このような監視対象機器は、図6のようなモデルにより表現できる。このモデルにおいては、監視対象機器は2つのインタフェースAおよびBを持ち、それぞれのインタフェースにおける単位時間当たりの受信トラフィック量 (y_{in-A} , y_{in-B}) と送信トラフィック量 (y_{out-A} , y_{out-B}) がトラフィック流量情報として取得される。

【0030】

また、ルータの内部には、トラフィックの終点や始点に対応する仮想的な点Oがあるものとし、 α ($\alpha \in \{A, B, O\}$) を始点とし β ($\beta \in \{A, B, O\}$) を終点として流れるトラフィックの量は $x_{\alpha\beta}$ と記されるものとする。この場合も、図5のモデルの場合と同様に、 $x_{\alpha\beta}$ を未知数とする連立方程式からTraffic Matrix Estimation により各 $x_{\alpha\beta}$ の値が推定される。

【0031】

図7は、本発明を実施するための別のネットワーク構成の例を示している。図7のネットワーク構成において、通信ネットワーク701は、監視対象機器711、712、およびネットワーク監視装置713を含み、通信ネットワーク702は、監視対象機器721およびネットワーク監視装置722を含み、通信ネットワーク703は、監視対象機器731、732、733、およびネットワーク監視装置734を含む。

【0032】

障害検出装置704は、通信ネットワーク701、702、および703の外部に設けられ、図8に示すように、トラフィック流量記録装置801、トラフィック流量分析装置802、異常トラフィック量計算装置803、および障害判定装置804を備える。

【0033】

ネットワーク監視装置713、722、および734はそれぞれ、図9に示すように、トラフィック流量取得装置901およびトラフィック流量記録装置902を備え、各ネットワーク内の監視対象機器からトラフィック流量情報を取得して障害検出装置704に送信する。そして、障害検出装置704は、各ネットワーク監視装置から送信されたトラフィック流量情報を用いて各ネットワーク内部の障害を検出する。

【0034】

図8のトラフィック流量記録装置801、トラフィック流量分析装置802、異常トラフィック量計算装置803、および障害判定装置804の機能は、基本的に、図3のトラフィック流量記録装置312、トラフィック流量分析装置313、異常トラフィック量計算装置314、および障害判定装置315の機能と同様である。また、図9のトラフィック流量取得装置901およびトラフィック流量記録装置902の機能は、基本的に、図3のトラフィック流量取得装置311およびトラフィック流量記録装置312の機能と同様である。

【0035】

このようなネットワーク構成は、セキュリティ等の理由により、監視対象機器が配置されているネットワークの外部からそのネットワークの内部へのアクセスが困難な場合に、有効である。このような構成であれば、障害検出装置704は、それぞれのネットワーク内部に配置されているネットワーク監視装置から送られてくるトラフィック流量情報を記録すればよい。したがって、障害検出装置704自身がそれぞれの監視対象機器と直接通信不可能であっても、それらの監視対象機器における障害発生の有無を判断することが可能である。

【0036】

ところで、図3および図8の障害検出装置と、図9のネットワーク監視装置は、例えば、図10に示すような情報処理装置（コンピュータ）を用いて構成することができる。図10の情報処理装置は、CPU（中央処理装置）1001、メモリ1002、入力装置1003、出力装置1004、外部記憶装置1005、媒体駆動装置1006、ネットワーク接続装置1007を備え、それらはバス1008により互いに接続されている。

【0037】

メモリ 1002 は、例えば、ROM (read only memory)、RAM (random access memory) 等を含み、処理に用いられるプログラムおよびデータを格納する。CPU 1001 は、メモリ 1002 を利用してプログラムを実行することにより、必要な処理を行う。

【0038】

図 3 のトラフィック流量記録装置 312、図 8 のトラフィック流量記録装置 801、および図 9 のトラフィック流量記録装置 902 は、メモリ 1002 に対応する。また、図 3 のトラフィック流量取得装置 311、トラフィック流量分析装置 313、異常トラフィック量計算装置 314、障害判定装置 315、図 8 のトラフィック流量分析装置 802、異常トラフィック量計算装置 803、障害判定装置 804、および図 9 のトラフィック流量取得装置 901 は、メモリ 1002 に格納されたプログラムを実行することにより実現される機能に対応する。

【0039】

入力装置 1003 は、例えば、キーボード、ポインティングデバイス、タッチパネル等であり、ネットワーク管理者等のオペレータからの指示や情報の入力に用いられる。出力装置 1004 は、例えば、ディスプレイ、プリンタ、スピーカ等であり、オペレータへの問い合わせ、アラーム、処理結果等の出力に用いられる。

【0040】

外部記憶装置 1005 は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク装置、テープ装置等である。情報処理装置は、この外部記憶装置 1005 に、上記プログラムおよびデータを格納しておき、必要に応じて、それらをメモリ 1002 にロードして使用する。

【0041】

媒体駆動装置 1006 は、可搬記録媒体 1009 を駆動し、その記録内容にアクセスする。可搬記録媒体 1009 は、メモリカード、フレキシブルディスク、CD-ROM (compact disk read only memory)、光ディスク、光磁気ディスク等の任意のコンピュータ読み取り可能な記録媒体である。オペレータは、この可搬記録媒体 1009 に上記プログラムおよびデータを格納しておき、必要に応じて、それらをメモリ 1002 にロードして使用する。

【0042】

ネットワーク接続装置 1007 は、LAN (local area network)、インターネット等の任意の通信ネットワークに接続され、通信に伴うデータ変換を行う。情報処理装置は、必要に応じて、上記プログラムおよびデータを外部の装置からネットワーク接続装置 1007 を介して受け取り、それらをメモリ 1002 にロードして使用する。

【0043】

図 11 は、図 10 の情報処理装置にプログラムおよびデータを供給することのできるコンピュータ読み取り可能な記録媒体を示している。可搬記録媒体 1009 やサーバ 1101 のデータベース 1103 に格納されたプログラムおよびデータは、情報処理装置 1102 のメモリ 1002 にロードされる。サーバ 1101 は、そのプログラムおよびデータを搬送する搬送信号を生成し、ネットワーク上の任意の伝送媒体を介して情報処理装置 1102 に送信する。CPU 1001 は、そのデータを用いてそのプログラムを実行し、必要な処理を行う。

【0044】

(付記 1) 複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出する障害検出装置であって、

前記監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を格納する格納手段と、

前記トラフィック流量情報を用いて、前記監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、得られた流量を異常トラフィック量として出力する計算手段と、

前記異常トラフィック量を用いて前記ネットワーク障害が発生したか否かを判定し、判定結果を出力する判定手段と
を備えることを特徴とする障害検出装置。

【0045】

(付記2) 複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出するコンピュータのためのプログラムであって、

前記コンピュータの格納手段から、前記監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を取り出し、

前記トラフィック流量情報を用いて、前記監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、

得られた流量を異常トラフィック量として用いて前記ネットワーク障害が発生したか否かを判定する

処理を前記コンピュータに実行させることを特徴とするプログラム。

【0046】

(付記3) 前記監視対象機器により生成されて出力されるデータのトラフィック量と、該監視対象機器により廃棄されるデータのトラフィック量と、該監視対象機器のインタフェースにより受信された後に同じインタフェースから送信されるデータのトラフィック量のうち少なくとも1つのトラフィック量を、前記異常トラフィック量として計算する処理を前記コンピュータに実行させることを特徴とする付記2記載のプログラム。

【0047】

(付記4) 前記監視対象機器の内部におけるトラフィックの総量に対する前記異常トラフィック量の比率を求め、該異常トラフィック量の比率が所定の閾値より大きい場合に前記ネットワーク障害が発生したと判定する処理を前記コンピュータに実行させることを特徴とする付記2記載のプログラム。

【0048】

(付記5) 前記監視対象機器の内部にトラフィックの終点および始点を表す仮想点を設け、該監視対象機器の内部において各インタフェースを始点とし他のインタフェースを終点とする第1のトラフィックの流量と、各インタフェースを始点とし該仮想点を終点とする第2のトラフィックの流量と、該仮想点を始点とし各インタフェースを終点とする第3のトラフィックの流量と、該監視対象機器の内部において各インタフェースを始点とし同じインタフェースを終点とする第4のトラフィックの流量を計算し、該第2、第3、および第4のトラフィックの流量の総量を前記異常トラフィック量として計算する処理を前記コンピュータに実行させることを特徴とする付記2記載のプログラム。

【0049】

(付記6) 前記第1、第2、第3、および第4のトラフィックの流量の総量に対する前記異常トラフィック量の比率を求め、該異常トラフィック量の比率が所定の閾値より大きい場合に前記ネットワーク障害が発生したと判定する処理を前記コンピュータに実行させることを特徴とする付記5記載のプログラム。

【0050】

(付記7) 前記トラフィック流量情報から前記第1、第2、第3、および第4のトラフィックの流量を推定する処理を前記コンピュータに実行させることを特徴とする付記5記載のプログラム。

【0051】

(付記8) 前記監視対象機器から前記トラフィック流量情報を取得して前記格納手段に格納する処理を前記コンピュータにさらに実行させることを特徴とする付記2記載のプログラム。

【0052】

(付記9) 前記ネットワーク障害が発生したと判定したとき、アラームを出力する処理を前記コンピュータにさらに実行させることを特徴とする付記2記載のプログラム。

【0053】

(付記10) 複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出するコンピュータのためのプログラムを記録した記録媒体であって、

前記プログラムは、

前記コンピュータの格納手段から、前記監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を取り出し、

前記トラフィック流量情報を用いて、前記監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、

得られた流量を異常トラフィック量として用いて前記ネットワーク障害が発生したか否かを判定する

処理を前記コンピュータに実行させることを特徴とするコンピュータ読み取り可能な記録媒体。

【0054】

(付記11) 複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出するコンピュータのためのプログラムを搬送する搬送信号であって、

前記プログラムは、

前記コンピュータの格納手段から、前記監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を取り出し、

前記トラフィック流量情報を用いて、前記監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、

得られた流量を異常トラフィック量として用いて前記ネットワーク障害が発生したか否かを判定する

処理を前記コンピュータに実行させることを特徴とする搬送信号。

【0055】

(付記12) 複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出する障害検出方法であって、

前記監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を用いて、前記監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、

得られた流量を異常トラフィック量として用いて前記ネットワーク障害が発生したか否かを判定する

ことを特徴とする障害検出方法。

【図面の簡単な説明】

【0056】

【図1】 本発明の障害検出装置の原理図である。

【図2】 第1のネットワーク構成を示す図である。

【図3】 第1の障害検出装置の構成図である。

【図4】 障害検出処理のフローチャートである。

【図5】 第1の監視対象機器のモデルを示す図である。

【図6】 第2の監視対象機器のモデルを示す図である。

【図7】 第2のネットワーク構成を示す図である。

【図8】 第2の障害検出装置の構成図である。

【図9】 ネットワーク監視装置の構成図である。

【図10】 情報処理装置の構成図である。

【図11】 記録媒体を示す図である。

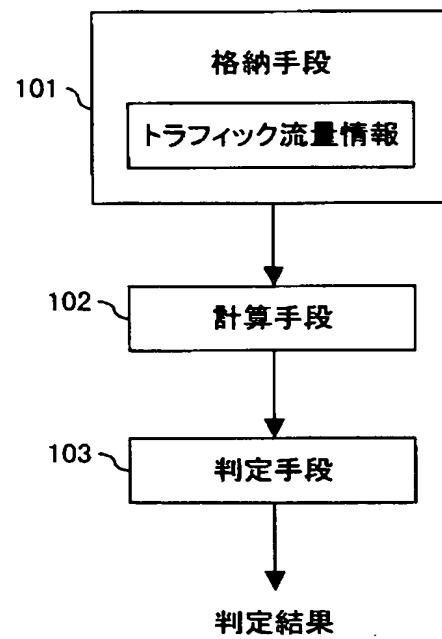
【符号の説明】

【0057】

101 格納手段
102 計算手段
103 判定手段
201、704 障害検出装置
202、203、204、205、206、207、301、711、712、721
、731、732、733 監視対象機器
713、722、734 ネットワーク監視装置
311、901 トラフィック流量取得装置
312、801、902 トラフィック流量記録装置
313、802 トラフィック流量分析装置
314、803 異常トラフィック量計算装置
315、804 障害判定装置
1001 CPU
1002 メモリ
1003 入力装置
1004 出力装置
1005 外部記憶装置
1006 媒体駆動装置
1007 ネットワーク接続装置
1008 バス
1009 可搬記録媒体
1101 サーバ
1102 情報処理装置
1103 データベース

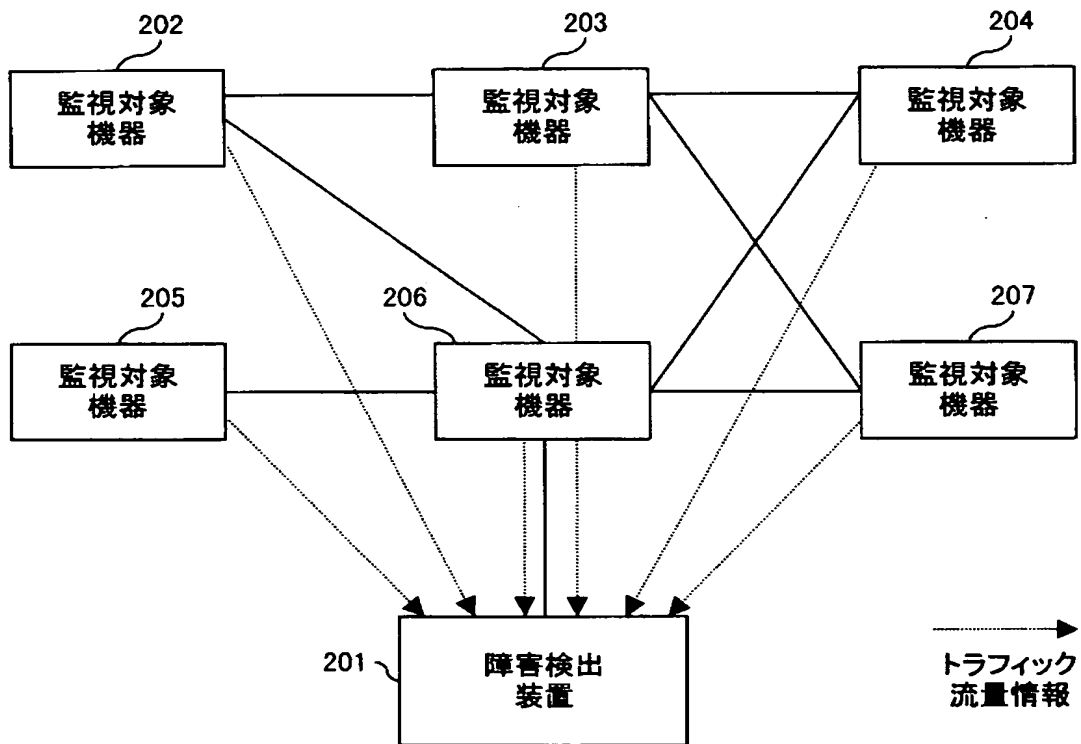
【書類名】 図面
【図 1】

本発明の障害検出装置の原理図



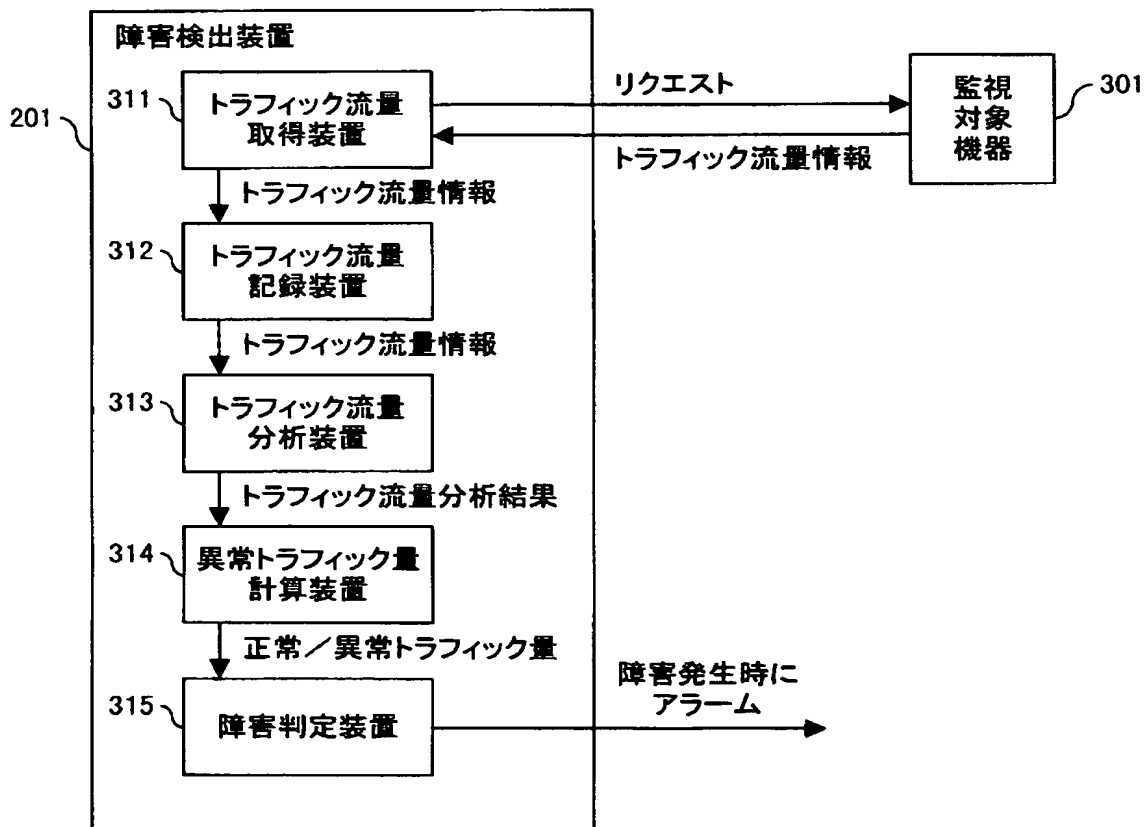
【図 2】

第1のネットワーク構成を示す図



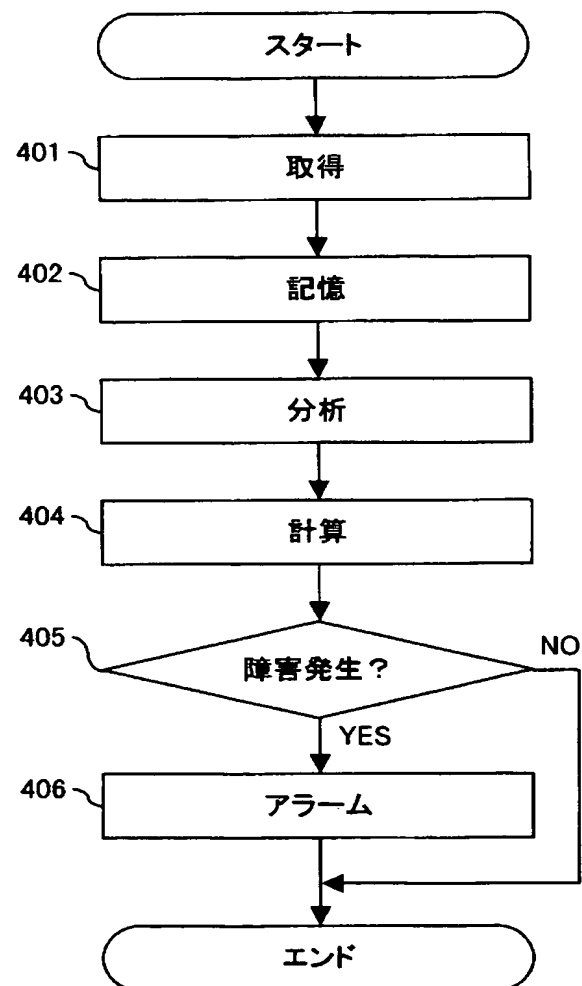
【図 3】

第1の障害検出装置の構成図



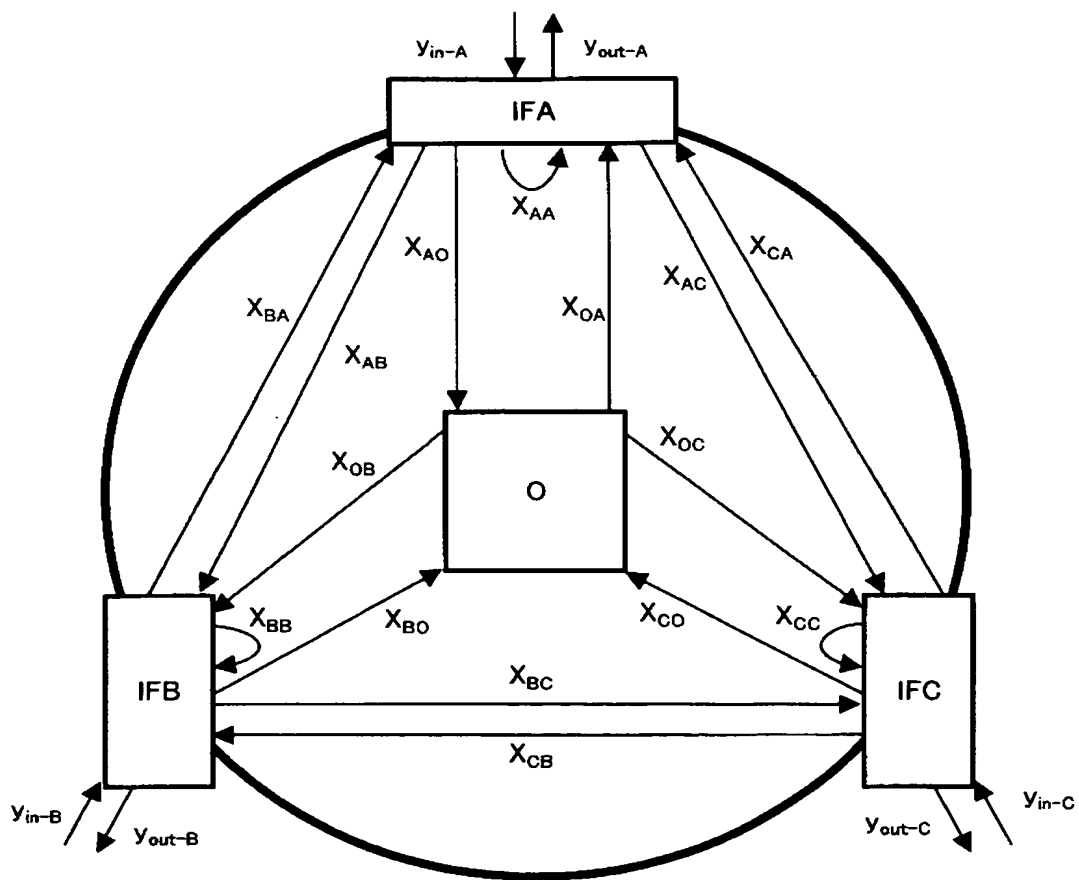
【図 4】

障害検出処理のフローチャート



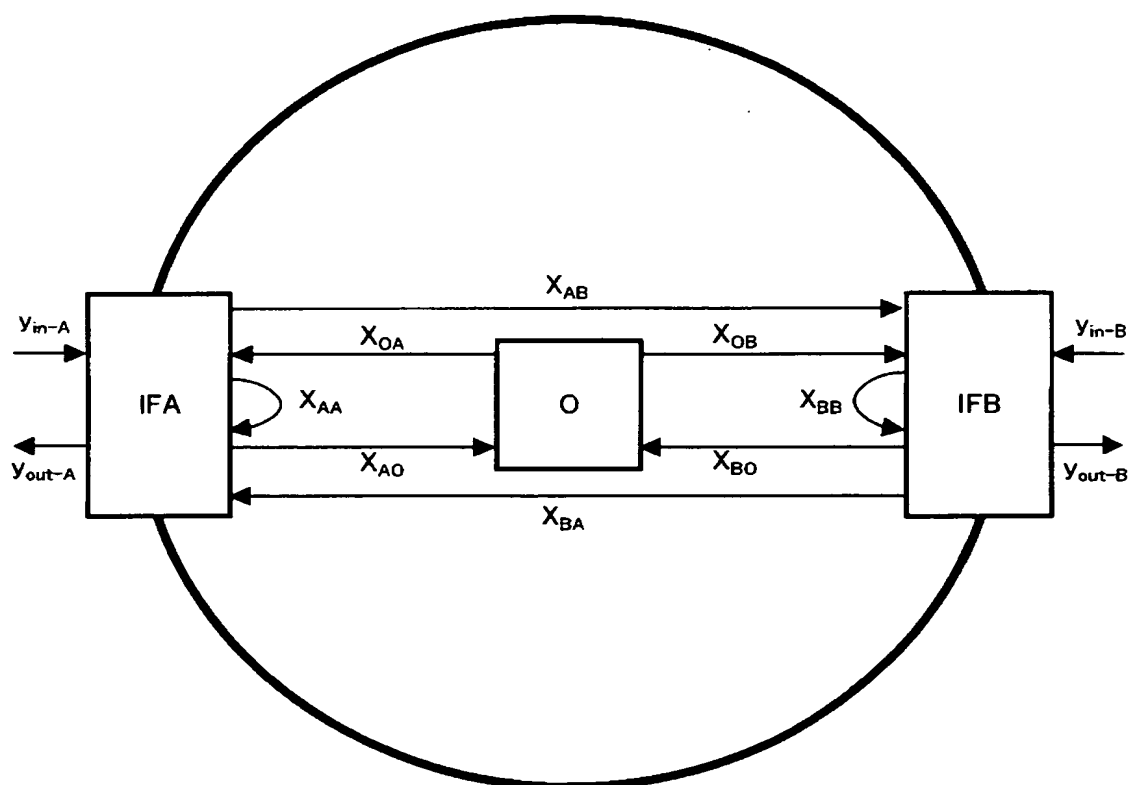
【図 5】

第1の監視対象機器のモデルを示す図



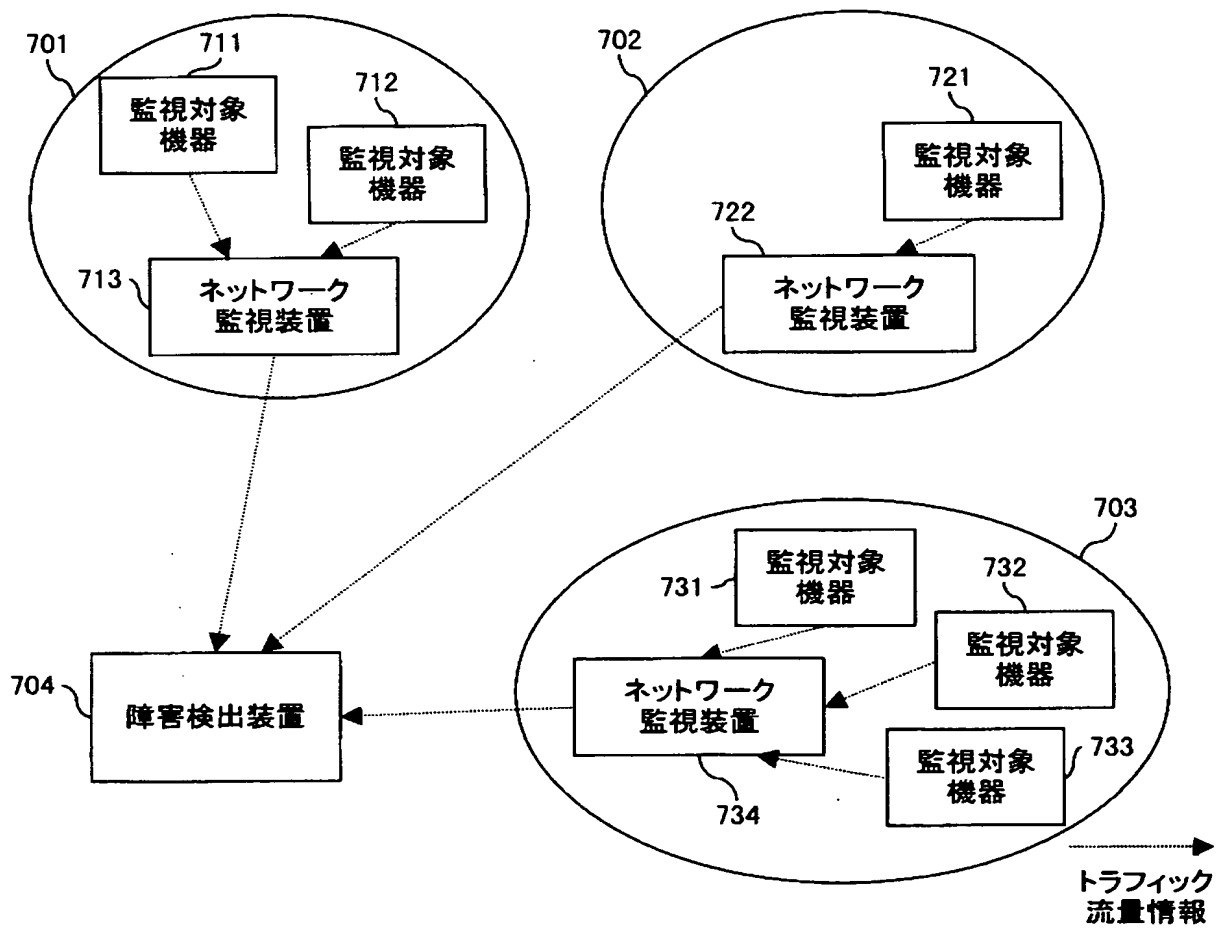
【図 6】

第2の監視対象機器のモデルを示す図



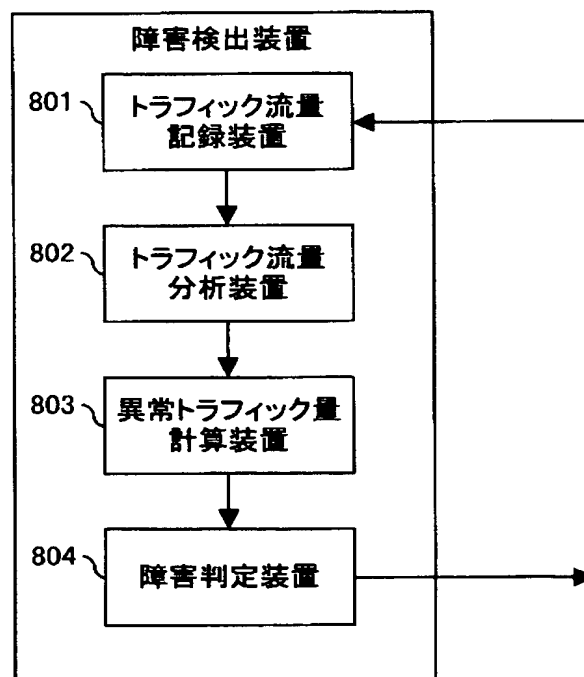
【図 7】

第2のネットワーク構成を示す図



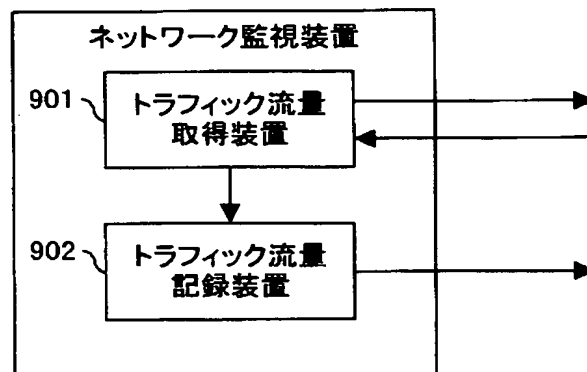
【図 8】

第2の障害検出装置の構成図



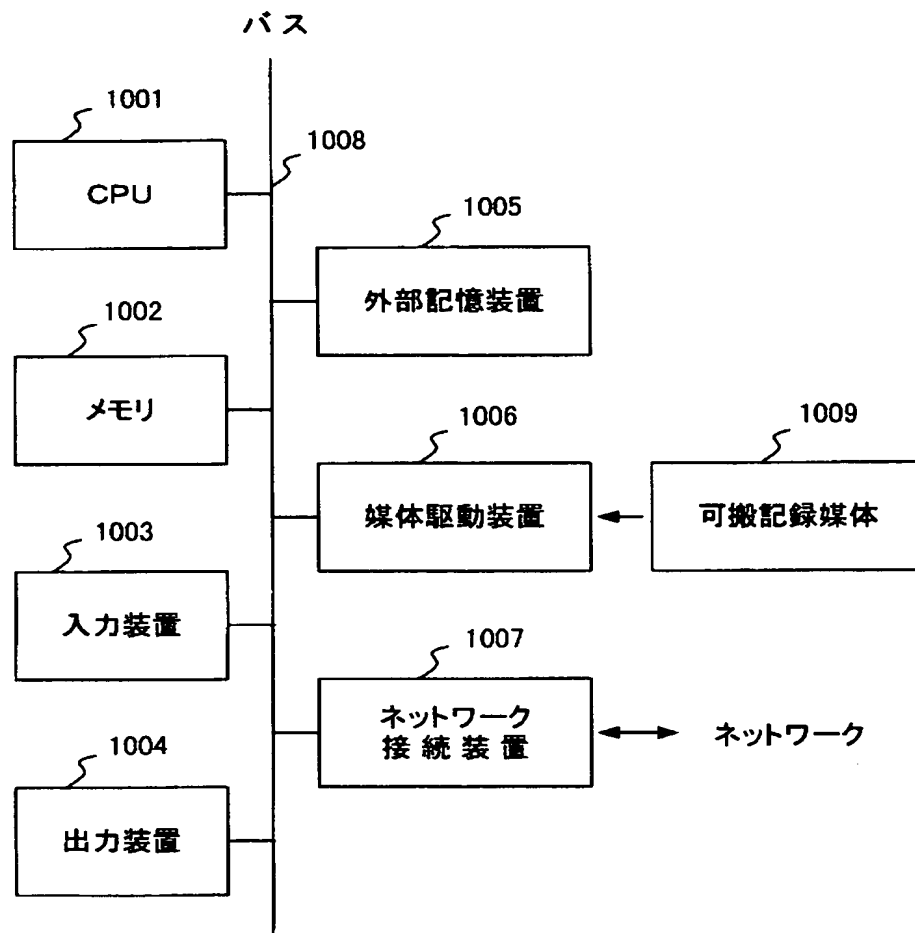
【図 9】

ネットワーク監視装置の構成図



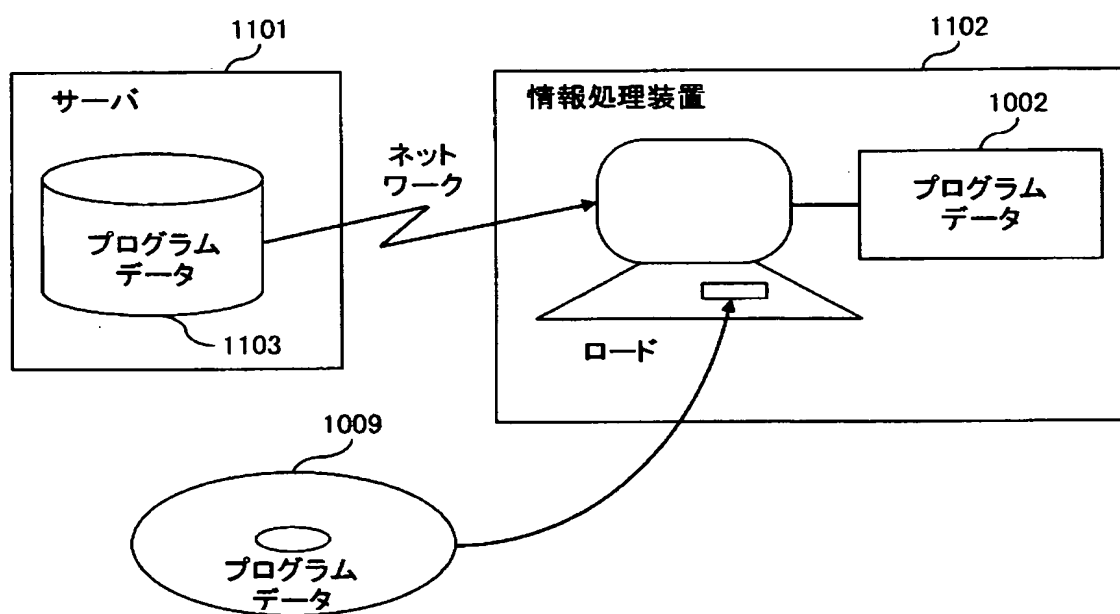
【図 10】

情報処理装置の構成図



【図 11】

記録媒体を示す図



【書類名】 要約書

【要約】

【課題】 通信ネットワーク内で発生する障害を、その影響が比較的小さい早期のうちに低コストで検出する。

【解決手段】 障害検出装置 2 0 1 は、通信ネットワーク内に配置された各監視対象機器から、その機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を取得する。そして、監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、得られた流量を用いてネットワーク障害が発生したか否かを判定する。

【選択図】 図 2



特願 2 0 0 3 - 2 9 6 7 6 8

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 2 2 3]

1 . 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社